International Journal of Computer Networking,
Wireless and Mobile Communications (IJCNWMC)
ISSN (P): 2250-1568; ISSN (E): 2278-9448
Vol. 8, Issue 1, Jun 2018, 1-10

INTERNET OF THINGS: A REVIEW ON ARCHITECTURE, SECURITY THREATS AND COUNTERMEASURES

PRIYA MAIDAMWAR, NEKITA CHAVHAN & UMA YADAV

Assistant Professor, Department of Computer Science & Engineering,

G H. Raisoni College of Engineering, Nagpur, India

ABSTRACT

Internet of Things also referred to as a distributed network of heterogeneous devices, provides the ability for humans to learn and interact with internet connected objects. Integration of these smart devices into standard internet introduces several security threats and attacks to our privacy. This paper presents an overview of IOT architecture, various attacks in each layer and possible countermeasures and further research objectives.

KEYWORDS: Internet of things, Security Issues, Privacy & Countermeasures

Received: Mar 09, 2018**; Accepted:** Mar 30, 2018**; Published:** Apr 23, 2018**; Paper Id.:** IJCNWMCJUN20181

Original Article

INTRODUCTION

The term Internet of Things can be viewed as self-configuring the wireless network of sensors. "Things" in IOT cover a wide gathering of physical items that can convey, share information, and data to accomplish a shared objective in various zones and applications. The objective of IOT is to enhance our lifestyle by interconnecting intelligent devices around us. IOT has numerous execution spaces like agriculture, transportation, healthcare, smart homes, smart cities, smart transportation and infrastructure etc.

There are numerous application areas of IOT, going from individual to big business situations [1]. The applications in individual and social space empower the IOT clients to collaborate with their encompassing condition, and human clients to keep up and fabricate social connections. Another use of IOT is in transportation region, in which different keen streets, savvy autos, and shrewd movement signals give secure and advantageous transportation offices. The endeavors and ventures area incorporate the applications utilized as a part of the back, saving money, showcasing and so forth to empower distinctive entomb and intra exercises in associations. The last application space is the administration and utility checking part which incorporates agribusiness, reproducing, vitality administration, reusing operations, and so forth.

This survey paper is organized as follows. Section II depicts the four-layer IOT structure and design. Section III manages the security issues identified with various security standards and the idea of IOT gadgets are introduced. The section likewise depicts the security issues that are related to each layer of IOT. Section IV discusses about the latest research that endeavors to address the security issues in IOT by a few countermeasures. Section V tends to the future headings that can be taken in light of the present status of IOT security. In the end, the paper is concluded in Section VI

ARCHITECTURE OF IOT

PERCEPTION LAYER

Physical layer manages the physical condition and gathers all the information acquired from the environment through of sensor hubs and other physical gadgets. This layer is in charge of correspondence between different physical gadgets. The objective of this layer is to provide authentication of devices and services to upper layers. The fundamental components of [9] physical layer include Arduino, ZigBee, Barcodes, RFID and all other sorts of sensors. Every gadget in IOT framework must have a one of a kind label which enables solid association with the system and generally, Universally Unique identifiers (UUID) are utilized as a part of the entire system by different gadgets. Consistently a gadget can be associated with numerous sensor hubs with one of a kind ID. Network layer conveys the transmitted data and forwards to a central system.

NETWORK LAYER

Network layer is in charge of correspondence between diverse physical gadgets, an organization of the system and besides upkeep of information through various correspondence conventions in an IOT structure. There isn't yet any fix convention for IOT however widely utilized protocol is MQTT and CoAP (Constrained Application Protocol). With the assistance of Wireless Sensors, the essential focus of this layer is to assemble information which is given from physical layer which is sent to a central processing unit. Every gadget in the IOT sends its private information with the help of remote sensors [10]. The network layer carries exchanging of data on the system of IOT. Thus secure and reliable exchange of information is done by this layer from perception layer towards different layers.

PROCESSING LAYER

The function of processing layer is to merge the services of, perception and network layer. Because of the substantial measure of information, it is exceptionally basic to store and process this information through databases for storage purposes. This layer performs intelligent computing in which it evaluates and processes collected data [2]. Henceforth entire intelligent processing function and ubiquitous computing is performed in this layer which is beginning innovation in this layer, so future advances of this layer will more appropriate for IOT. Hence, the development of future innovations of this layer will be useful for the advancement of IOT framework.

APPLICATION LAYER

Application layer gives administrations as indicated by client request. The handled data of the lower layers is used to create useful services for the end client. The data gives a stage for such applications which could profit the client from multiple points of view, for example, education, smart homes, transportation, and smart hospitals and so on. The data security in IOT should be associated with security features like confidentiality, integrity, identification [4].

Application Layer (Intelligent Devices/Applications/Systems)
Processing Layer (Databases, Storage Components)
Network Layer (Wired/Wireless Components, Desktops)
Perception Layer (Sensor Nodes, RFID Tags, Smart Card)

Figure 1: Four Layer IOT Framework

SECURITY ATTACKS AT DIFFERENT LAYERS PERCEPTION LAYER ATTACKS

HARDWARE TAMPERING

This sort of assault may attack the sensor hub or damage it by physically sending and getting a complete hub or part of the equipment or even analyze the hubs electronically to get access and alter touchy data [12]. For Example:- Changing the electronic combination or by catching the passage hub, the assailant can get all the data on that system including steering table, correspondence key, cryptographic key, radio key and so forth and danger all the system counting higher layers.

NODE CAPTURE ATTACK

The aggressor can infuse a fake hub between the hubs of the system [7] consequently the assailant gain access and have the capacity to control the whole network of the information. It can make the hub to quit transmitting the genuine information and henceforth destroy the whole system.

REPLAY ATTACK

A replay assault is a class of network assault in which an assailant distinguishes an information transmission and falsely has it duplicated or delayed. The duplicate or delay of the information transmission is completed by the sender or by the malicious element, who catches the information and retransmits it [8].

SLEEP DENIAL ATTACK

Hub on the remote places in IOT organize are for the most part fueled by replaceable batteries, the hubs are modified to rest when they are not being used to build their battery life [18]. In this assault, the aggressor keeps the hub alert and anticipate them to nod off by nourishing incorrectly contribution to the hub which comes about in control utilization subsequently the hub shutdown.

RF JAMMING

Intruder can deny the services just by sending noise signals over the network [2]. This noise interference can destroy the communication between the nodes.

TAG CLONING

The method of replacing the first tag with the new one and replicating unique label identifier to it [8]. The labels and programming are accessible in the market. The assailant can without much of a stretch replace the first tag with the better and brighter one, if no physical access protection is provided for RFID labels.

NETWORK LAYER ATTACKS

RFID UNAUTHORIZED ACCESS

In RFID frameworks, getting access of labels is simple for anybody in light of the fact that generally in the RFID framework it does not have the setup methodology or any framework of verification [6]. In this way, it obviously implies that aggressor can change, read or erase the data of sensor hubs.

MAN-IN-MIDDLE ATTACK

Web intruder interferes between the two sensor hubs to get too confined data and abuses the protection of nodes[23]. Such attack doesn't request the intruder to be physically available in the area of the system. This should be possible by utilizing the correspondence protocol of the IOT.

TRAFFIC ANALYSIS ATTACK

This category of assault is the essential security assault on the network layer while using any web program. The enemy can get to mystery data and other helpful information which are from RFID innovation on account of its remote quality. Before applying this assault the aggressor at first catche data and information about the associated arrange [25]. This work is achieving by utilizing a few sniffing operations such port sniffing applications, bundle checking applications and so forth.

RFID SPOOFING

In this assault, the adversary catches the information transmitted by spoofing RFID signals. At that point in order to make it credible the aggressor transmits his own data which have unique ID [24] of RFID tag, thus by appearing to be the genuine source, the adversary can get to the IOT framework.

SINKHOLE ATTACK

The aggressor produces a sinkhole and attracts all activity which is from the hubs of the wireless sensor network. Here in this assault, it harms the privacy and protection of information and thereby ceasing the transmission of packets [22] Instead of to sending it to goal, it denies the resources to the system.

PROCESSING LAYER ATTACKS

APPLICATION SECURITY

The majority of the application on cloud SAAS are conveyed through web i.e. web administrations. An aggressor can undoubtedly utilize the web to get into the IOT arrange and can take the information or can perform malicious exercises. Security issues in SAAS are much not quite the same as normal web securities issues. OWASP had distinguished diverse security issues on SAAS [3].

DATA SECURITY

Information security is the real worry of a SAAS client. It's the duty of the SAAS supplier to guarantee the security, the information prepared and put away on the cloud as plain content. The major security issues happen with the help of information reinforcement given by the service provider [2]. Information back is advertised through outsider in a large portion of the cases which increases the chances of data theft.

THIRD PARTY RELATIONSHIPS

PaaS not just provides programming languages, it also provides third-party web service component. Several sources of mashups are combined together which increases security issues like a system and information security.

VIRTUALIZATION THREATS

Virtual machine security is important as different machines and the occurrence of any harm to machine influences the other. In this layer, virtualization is extremely unreliable about numerous sorts of attacks [1].

APPLICATION LAYER ATTACKS

PHISHING ATTACK

In this sort of assault, the intruder can hijack sensitive data [16] and access all private information by ridiculing authorization credentials of the client. These assaults are used to take login certifications, credit card details and so on.

MALWARE, SPYWARE, VIRUS, WORMS

The intruder influences the arrangement of IOT by infusing malicious programming in the framework [11] which brings about changing results. These sorts of assaults hurt the framework by altering data, denying its administrations and get access to secret information.

MALICIOUS CODE

In the IOT framework generally, gadgets are associated and interacting with each other by means of the web. The system totally shuts down [13] when a client keeps tracking the gateway and runs the dynamic X content. This kind of scripting strikes web applications and thereby gains control on the system and steals the information.

DENIAL OF SERVICE

In this case, an intruder can influence all clients in a system of IOT framework by inserting DOS attack of the application layer and thereby unauthorized client can access frameworks data [15]. This kind of assault also hinders the authorized clients from communicating with the application layer.

SECURITY COUNTERMEASURES AT DIFFERENT LAYERS

PERCEPTION LAYER COUNTERMEASURES

PHYSICAL SECURITY

In Perception Layer majority of attacks are settled by outlining the gadgets those are secured physically. Design and planning of such units [17] like acquisition unit, radio frequency circuits and so forth are not supposed to be changed and also not to be of high quality. The architecture of antenna for wireless communication is physically secure and accordingly can impart over great separation over long detachment.

SECURITY RISK ASSESSMENT

Security Risk Assessment strategy gives security of information thereby maintaining a strategic distance from security ruptures in an IOT. [19]. It is basic for security viewpoint of IOT by finding diverse sorts of dangers to the system. Exactly when a mistake is found such security procedures then RFID runs an automatic kill label of RFID which ceases unapproved access to data.

SECURE BOOTING

The genuineness of the programming can be verified by applying the cryptographic hash algorithm. This algorithm authorizes the software running on the gadgets by digital signature [20]. Numerous cryptographic hash algorithms are impossible to implement as a result of low handling capacity on numerous gadgets. Some cryptographic hash algorithms, for example, NH and WH cryptographic calculation are reasonable to implement on few gadgets which require less use of energy.

INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is is a framework that screens organize a movement for suspicious action and issues alarms when such action is found [12].

DEVICE AUTHENTICATION

To keep malicious devices out of the IOT network, verification of the gadgets should be done before getting into the network[13]. Without appropriate authentication, the gadget should not be permitted to communicate with the system which prevents false information flow in the system.

IPSEC SECURE CHANNEL

IPSec Security channel has two kinds of secure functionalities, encryption, and verification which give security [2]. Hardware tampering and eavesdropping can be stopped by encryption which guarantees the privacy of information. The recipient can distinguish that the sender of the data onto IP is fake or genuine.

NETWORK LAYER COUNTERMEASURES

NETWORK LEVEL AUTHENTICATION

With the assistance of proper network authentication technique and encryption process, illegal access of the devices can be avoided. The Most popular attack is DoS attack which can influence the system by spreading pointless data.

POINT-TO POINT ENCRYPTION

Point to **point encryption** is a system for secure transfer of information where data is encrypted and decrypted only at the endpoints, no matter how many points it touches in the middle of its virtual journey. This type of encryption is a great way to provide secure, **private communication.**

GPS TRACKING SYSTEM

By introducing GPS framework into the gadget, spoofing attack can be encountered from network layer of the IOT system [6]. S. Daneshmand et al. proposed and developed the GPS location technique which is the best arrangement proposed yet.

PROCESSING LAYER COUNTERMEASURES

WEB APPLICATION SECURITY SCANNERS

This application is used for distinguishing different dangers [15] which is available in the front end of the web. Other web firewall applications, in addition, perceive the dangers of a potential aggressor.

FRAGMENTATION REPLICATION SCATTERING

In Fragmentation replication scattering the fundamental information stored on the cloud [4] is spitted into parts and allocates into allocates into various bits of limit in servers. The piece does not contain any helpful data about the information so the danger of information theft is limited in this situation.

HYPERSAFE

Hyper safe gives security to the memory pages from being changed and furthermore permits a limitation of pointing record that progressions observed information onto the pointer records [4].

HOMOMORPHIC ENCRYPTION

This sort of encryption performs computation on ciphertexts, creating an encoded result which, when unscrambled, matches the consequence of the tasks as though they had been performed on the plaintext. The reason for homomorphic encryption is to permit calculation of encoded information.

APPLICATION LAYER COUNTERMEASURES

BIOMETRICS AUTHENTICATION

This technique allows an individual to be verified and authenticate them based on a set of recognizable and identified data, which are specific and unique to them. The stored information is later compared to the individual biometric data to be verified. Here it is the individual identity which is being verified.

PROTECTIVE SOFTWARE

Programming which gives security, for example, anti-virus, anti-spyware are necessary for security, integrity, and reliability of the IOT network.

ACCESS CONTROL LISTS

Confidentiality of the network and data privacy is the essential part which can be maintained by setting up the principles and permits entrance and checking out of the network. It can be managed by monitoring access requests from many users thereby denying or allowing incoming or outgoing traffic in the IOT system.

CRYPTOGRAPHIC HASH FUNCTIONS

Hash functions can be utilized for various purposes, which incorporate data integrity checks, digital signature, validation, and different data security applications. A hash function accepts a string of any length as information and generates a fixed length string which can be used as a sort of "signature" for the information provided. Thus, a man knowing the "hash value" can't know the original message, yet just the individual who knows the original message can demonstrate the "hash value" is made from that message.

IOT Layer & its Components	Function of Layer	Security Issues it Addresses	Effects	Counter Measures
Perception Layer (Sensor nodes, RFID Tags, Smart Card)	Collection of Information from environment	Hardware Tampering	Manipulates sensitive information by destroying sensors	Physical Security
		Physical Damage	Damages components of hardware device	Risk Assessment
		Node Capture Attack	Attacker gain access to network & stop transmitting real data	Secure Booting
		Replay Attack	Injects malicious code & hence makes services unavailable	Intrusion detection System
		Sleep Denial Attack	Nodes are shutdown	Device Authentication
		RF Jamming	Communication is stopped due to distortion of signals	IPSec secure channel
		Tag Cloning	Replace original tag with new one	Device Authentication
Network layer (Wired or Wireless networks)	Routing and transmission of data to different IOT devices	RFID Unauthorized Access	Modify or delete complete information	Network Authentication
		Man-in-Middle Attack	Interference in communication between two nodes	Point-to Point Encryption
		Traffic Analysis Attack	Unauthorized access to sensitive information	Secure Routing
		RFID Spoofing	Intrusion in Network	GPS Location System
		Sink hole Attack	Drops all packets (Leakage of data)	Security aware adhoc Routing
		Routing Information Attacks	Sending false error messages by creating routing loops	Routing table Encryption
Processing layer (Databases)	Storage of data from lower layers to database	Application Security	Data is stolen from User cloud	Web Application Scanners
		Data Security	Leakage of confidential Information	Fragmentation redundancy scattering
		Underlying Infrastructure Security	Unable to access lower layer functions	Fragmentation redundancy scattering
		Third Party relationships	Data Leakage	Encryption
		Virtualization Threats	Damaging resources	Hypersafe
		Shared Resources	Unauthorized access to resources	Homomorphic Encryption
Application layer (Intelligent devices)	Intelligent devices provides services as per user demand	Phishing Attack	Captures sensitive information (Stealing user credentials)	Biometrics Authentication
		Virus, Worms, Trojan Horse, Spyware	Alteration of confidential data	Protective Software (Antivirus,Antispyware)
		Malicious Scripts	System shuts down (Resource hijacking)	Firewalls
		Denial of Service	Services are unavailable to authorized users	Access Control Lists
		Data Protection & Recovery	Loss of data	Cryptographic Hash Functions

FUTURE DIRECTIONS

By the year 2025 hundred millions gadgets are to be associated in the IOT. So the security of the system should be the most critical issue in up and coming days. The security is turning into a challenge on the grounds that there is no standard design and security techniques actualized for one design may not be feasible for another, accordingly likelihood of security attacks increases. In this way, the requirement for a standard engineering for IOT is mandatory. Hubs in an IOT organize are not fit enough to deal with complex security calculations like Cryptography and so forth henceforth there is a solid requirement for a few algorithms that can be implemented on these low-processing devices.

CONCLUSIONS

IOT has been a hot research theme throughout a previous couple of years what's more, as other progressive advances, it likewise faces numerous challenges, which are the security and protection dangers. In this paper, we depicted the working of four layers of IOT (Perception Layer, Network Layer, Processing Layer and Application Layer) and after that, we investigated various security dangers that can be encountered in these layers. Moreover, we clarified the countermeasures that can be embraced to counteract and secure the IOT organize from the security dangers. Besides, we additionally proposed a few changes in the IOT system to influence it more to secure and to overcome the deployment issues. Also, comparative analysis of security attacks and their preventive measures is presented in the table.

REFERENCES

1. *Mayuri A. Bhabad and Sudhir T. Bagade, "**Internet of Things: Architecture, Security Issues and Countermeasures**" International Journal of Computer Applications (0975 – 8887) Volume 125 – No.14, September 2015 pp 1 – 4.*
2. *Abdul Wahab Ahmed, Mian Muhammad Ahmed, Omair Ahmad Khan, Munam Ali Shah, "**A Comprehensive Analysis on the Security Threats and their Countermeasures of IOT**" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 7, 2017 pp 489 – 501.*
3. *Santhosh Krishna B V and Gnanasekaran T, " **A Systematic Study of Security Issues in Internet-of-Things (IOT)**" International conference on I-SMAC (IOT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017) pp 107-111.*

4. *Mian Muhammad, Munam Ali Shah, Abdul Wahid, "**IOT Security: A Layered Approach for Attacks & Defenses**" 2017 International Conference on Communication Technologies (ComTech), pp 104-110.*
5. *Zejun Ren, Xiangang Liu, Runguo Ye and Tao Zhang, "**Security and Privacy on Internet of Things**" in IEEE 2017 pp 140-144.*
6. *Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li_, and Hongbin Zhao, "**A Survey on Security and Privacy Issues in Internet-of-Things** ",IEEE INTERNET OF THINGS JOURNAL 2016, pp 1-16.*
7. *Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, "**Internet of Things (IOT) Security: Current Status, Challenges and Prospective Measures**" The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), pp 336 – 341.*
8. *Md Husamuddin and Mohammed Qayyum, "Internet of Things: A Study on Security and Privacy Threats", in IEEEJ 2017.*
9. *Arsalan Mohsen Nia and Niraj K. Jha, "**A Comprehensive Study of Security of Internet-of-Things** " in IEEE Transactions on Emerging Topics in Computing 2016 pp 1-16.*
10. *Alaba, Fadele Ayotunde, et al. "Internet of things Security: A Survey."Journal of Network and Computer Applications (2017).*
11. *Surapon Kraijak and Panwit Tuwanut, "A SURVEY ON IOT ARCHITECTURES, PROTOCOLS, APPLICATIONS, SECURITY, PRIVACY, REAL-WORLD IMPLEMENTATION AND FUTURE TRENDS".*
12. *Kai Zhao, LinaGe, "**A Survey on the Internet of Things Security**", 2013 Ninth International Conference on Computational Intelligence and Security, pp 663 -667.*
13. *Suchitra.C, Vandana C.P, "**Internet of Things and Security Issues**", International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 1, January 2016, pg.133 – 139.*
14. *Anne H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng, "**IOT Middleware: A Survey on Issues and Enabling Technologies"**, IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 1, FEBRUARY 2017, pp 1-20.*
15. *I. Andrea, C. Chrysostomou, and G. Hadjichristofi, **"Internet of Things: Security Vulnerabilities and Challenges,"** in International Workshop on Smart City and Ubiquitous Computing Applications,2015, pp. 180–187.*
16. *A. Tewari, A. K. Jain, and B. B. Gupta, **"Recent survey of various defense mechanisms against phishing attacks,"** J. Inf. Priv. Secur.ISSN, vol. 6548, no. Feb, pp. 3–13, 2016.*
17. *H. Tobias and E. Al., "Security Challenges in the IP-based Internet of Things," 2011.*
18. *SAXENA, ROHIT, et al. "GOOGLE GLASS AND GLASSWARE DEVELOPMENT USING REST ARCHITECTURE."*
19. *T. Bhattasali, "Sleep Deprivation Attack Detection in Wireless SensorNetwork," Found. Comput. Sci. New York, USA, 2012.*
20. *M. C. M and A. Serbanati, "An overview of privacy and security issues in the internet of things," Springer, 2010.*
21. *D. Raggett, **"The Web of Things: Challenges and opportunities,"** IEEE Comput., vol. 48, no. 5, pp. 26–32, May 2015.*
22. *L. Yao, Q. Z. Sheng, and S. Dustdar, **"Web-based management of the Internet of Things,"** IEEE Internet Comput., vol. 19, no. 4, pp. 60–67, Jul./Aug. 2015.*
23. *Y. Qin et al., **"When things matter: A survey on data-centric Internet of Things,"** J. Netw. Comput. Appl., vol. 64, pp. 137–153, Feb. 2016.*

24. *Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash* ***— "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications",*** *IEEE communication surveys & tutorials, vol. 17, no. 4, fourth quarter 2015.*

25. *U. Farooq M, Waseem M, Mazhar S, et al.* ***"A Review on Internet of Things".*** *(IOT)[J]. International Journal of Computer Applications, 2015 pp1-7.*

26. *L. Li,* ***"Study on Security Architecture in the Internet of Things,"*** *in International Conference on Measurement, Information and Control (MIC) Study, 2012, no. Mic, pp. 374–377*